(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 041 481 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
04.10.2000 Bulletin 2000/40

(51) Int. Cl.[7]: **G06F 1/00**, G06F 17/60

(21) Application number: **00104285.2**

(22) Date of filing: **01.03.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **31.03.1999 JP 9127399**

(71) Applicant: **Hitachi, Ltd.**
Chiyoda-ku, Tokyo 101-8010 (JP)

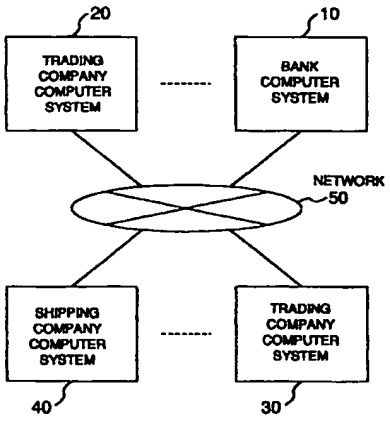
(72) Inventors:
- **Kitajima, Tetsuya,**
  Hitachi,Ltd.,
  Intell.Prop.Group
  Chiyoda-ku, Tokyo 100-8220 (JP)
- **Kawatsura, Yoshiaki,**
  Hitachi,Ltd.,
  IntellPropGroup
  Chiyoda-ku, Tokyo 100-8220 (JP)
- **Chiba, Hiroyuki,**
  Hitachi,Ltd.,
  Intell. Prop. Group
  Chiyoda-ku, Tokyo 100-8220 (JP)

(74) Representative:
Strehl Schübel-Hopf & Partner
Maximilianstrasse 54
80538 München (DE)

(54) Data interchange method and system

(57) Data interchange method and apparatus for enabling an interchange of digital data which is performed among a plurality of parties (10, 20, 30, 40) to be executed without intervening a center system or the like as a third party while assuring the contents of the digital data. When data is transmitted between two parties who transmit and receive the data, a right assignor of the data makes his own digital signature, assures the contents of the data, and transmits the data. A right assignee of the data confirms the contents of the data and the right assignor, subsequently makes his digital signature to the data, and transmits the data to the right assignor. The right assignor checks the data assignee, makes his own digital signature to the data and transfers the right of the data to the assignee, thereby executing the interchange of the data between the two parties.

FIG. 1



EP 1 041 481 A2

Description

BACKGROUND OF THE INVENTION

[0001] The present invention relates to a data interchange method for interchanging digital data between systems of two parties via a network or a digital medium and to, a system to which such a method is applied. More particularly, the invention relates to a data interchange method suitable for mutually checking and safely interchanging digital data of a digital document or the like which is circulated among a plurality of parties, a system to which such a method is applied and a data interchange executing program recording medium.

[0002] In recent years, owing to the progress of an information processing technique, for example, in various trades, a demand such that a document which is interchanged between trading parties is replaced with digital document data and the digital document data is interchanged between the parties via a digital medium such as a network to thereby perform the trade has been widespread.

[0003] For example, also in the field of trade and finance, digitization of a document which is interchanged between the trading parties is examined. The interchange of the document between the parties concerned with the document in the trade and finance can be divided into two kinds and considered due to the nature. One is an interchange of a document as information and the other is an interchange of a document in which transmutation has to be managed.

[0004] As a document in which the transmutation has to be managed, for example, there is a bill of lading (hereinafter, abbreviated to B/L) on which information for freight or cargo loaded in a ship by a shipping company has correctly been recorded. The B/L is a bill which can be interchanged with the freight at an importing place of the freight and denotes valuable papers for authenticating the owner of the freight and a duty of a payment for the freight at any time point of the import and export. The B/L is formed by using a sheet of paper as a medium in the present situation. A party who possesses the original of papers can own the right as valuable papers. When it is considered to realize the B/L as digital data, a technique to correctly assure the transmutation while the digitized B/L is circulated is necessary.

[0005] As one of well-known techniques to interchange digital data, there is a technique disclosed in, for example, JP-A-9-251502. The technique to pay data having a money value, namely, digital money is disclosed in JP-A-9-251502. In this case, a payer authorized by some certificate authority adds his own digital signature to data (digital money) to be interchanged and transmits it to a partner, thereby assuring the contents of the data to be transmitted.

[0006] In JP-B-8-27812, a technique such that digital data as transaction information is checked by two parties, digital seal information indicative of agreement with the transaction contents is mutually interchanged, and the two parties have the information together with digital data, thereby assuring the transaction itself is disclosed. According to the technique disclosed here, a receiver of the digital data forms a compression cryptogram of the received digital data and returns a part of it as tally information to a transmitter. The transmitter checks the tally information and transmits his own tally information to the receiver. After that, the receiver checks the tally information of the transmitter and transmits his own tally information to the transmitter. Consequently, even if the receiver denies a fact of the transaction and runs away with the digital seal of the transmitter without returning the digital seal of the receiver to the transmitter, the transmitter uses the received tally information as an evidence, thereby enabling the digital transaction to be assured.

SUMMARY OF THE INVENTION

[0007] According to the technique disclosed in the foregoing JP-A-9-251502, by adding the digital signature of the transmitter to the data and transmitting the resultant data to a partner, the transmitter assures its contents. It is now considered that the method is applied to the interchange of a concerned document in the trade and finance. In this case, in order to prevent an unauthentic act for the data with the digital signature transmitted by the transmitter, for example, such an act that after the reception is refused, the received data is circulated, the receiver cannot refuse the reception of the data. Therefore, the receiver cannot perform the operation such that he checks the contents of the transmitted data and judges whether he receives it or not, so that there is a possibility such that the defective data is received. In case of the B/L, in the present situation, if only a part of the B/L is different from that formed by the shipping company, it cannot be interchanged with cargo. Accordingly, the receiver has a large risk.

[0008] In addition, according to the technique, double payment by the payer is tried to be avoided by criminal and social sanctions after the revelation of the unauthentication. However, it is impossible to prevent a third party in good faith from being damaged. In the trading transaction, such a situation results in a fatal defect.

[0009] When it is considered that the technique disclosed in JP-B-8-27812 is applied to the interchange of the concerned document in the trade and finance, it is difficult to unconditionally identify the owner from the data to be interchanged, so that the data cannot be transferred as a right. If a process for adding the contents of the interchange such as names or the like of the transaction parties who perform the transaction to the data to be interchanged is performed, it is considered that the owner can be identified from the data even by the technique disclosed in JP-B-8-27812. Generally, the

B/L is circulated among at least three parties. In consideration of it, when data is interchanged, it is necessary that a data forming person has to form data by inserting the names of all of the concerning parties among which the data is circulated. It obstructs the circulation performance of the B/L as valuable papers, so that a mechanism of the trading transaction business itself is obstructed. In order to interchange the trading document concerned, therefore, the technique disclosed in JP-B-8-27812 cannot be substantially applied.

[0010] It is an object of the invention to provide a data interchange method which can interchange digital data among a plurality of parties while its contents are assured, a system to which such a method is applied, and a program recording medium for embodying such method and system.

[0011] Another object of the invention is to provide a data interchange method whereby digital data can be interchanged among a plurality of parties without passing through a center system or the like as a third party, and a system to which such a method is applied, and a program recording medium for embodying such method and program.

[0012] To accomplish the above objects, according to one aspect of the invention, there is provided a data interchange method for interchanging data among a plurality of computers through a network or a digital medium, comprising the following steps. In a first computer serving as a transmitting source of data, a first message obtained by adding a first digital signature to indicate the validation or authentication of the data to the data is formed and transferred to a second computer. In the second computer, the validation of the first message is checked on the basis of the first digital signature. In the second computer, a second message is formed by adding a second digital signature to indicate the validation to the first message and transferred to the first computer. In the first computer, the validation of the second message is checked on the basis of the second digital signature, and a third message is formed by adding a third digital signature to indicate the validation to the second message and transferred to the second computer. In the second computer, the validation of the third message is checked on the basis of the third digital signature and the third message is held as data to be received from the first computer.

[0013] According to the aspect of the invention, in the process for forming the second message, data included in the first message is outputted to an output unit and the second message is formed in accordance with information which is inputted from an input unit in response to the output of the data.

[0014] Information of validation indicating that the transmitting source is the first computer is added to the first message. Similarly, information of validation indicating that the transmitting source is the second computer is added to the second message.

[0015] According to another aspect of the invention, further in the second computer, a fourth message is formed by adding a fourth digital signature to indicate the validation of the third message to the third message and transferred to a third computer. In the third computer, the validation of the fourth message is checked on the basis of the digital signature included in the fourth message and a fifth message is formed by adding a fifth digital signature to indicate the validation to the fourth message and transferred to the second computer. In the second computer, the validation of the fifth message is checked on the basis of the fifth digital signature and a sixth message is formed by adding a sixth digital signature to indicate the validation to the fifth message and transferred to the third computer. In the third computer, the validation of the sixth message is checked on the basis of the sixth digital signature and the sixth message is held as data to be received from the second computer.

[0016] According to still another aspect of the invention, in the second computer, a fourth message to be transferred to a third computer is formed on the basis of the third message and transferred to a third computer. In the third computer, a fifth message is formed by adding a fourth digital signature to indicate the validation to data except for the third digital signature included in the fourth message and transferred to the second computer. In the second computer, the validation of the fifth message is checked on the basis of the fourth digital signature and a sixth message is formed by adding a fifth digital signature to indicate the validation to the fifth message and transferred to the third computer. In the third computer, the validation of the sixth message is checked on the basis of the fifth digital signature and the sixth message is held as data to be received from the second computer.

[0017] Other objects, features and advantages of the present invention will become apparent from the description of the following embodiments of the invention taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018]

Fig. 1 is a block diagram showing a construction of a trade and finance system in an embodiment of a data interchange system to which a data interchange method according to the invention is applied;

Fig. 2 is a block diagram showing a construction of a computer system which is connected to the trade and finance system;

Fig. 3 is a block diagram of an IC card for use in interchange of a B/L and its holding;

Fig. 4 is a flowchart showing a flow of processes which are executed when the B/L is transferred from a computer system on the occurring source

side of the B/L to another computer system;

Fig. 5 is a detailed flowchart for a generating process of a B/L message;

Fig. 6 is a data constructional diagram showing a format of the B/L message;

Fig. 7 is a detailed flowchart for a generating process of an agreement message;

Fig. 8 is a data constructional diagram showing a format of the agreement message;

Fig. 9 is a detailed flowchart for a generating process of an assignment assuring message;

Fig. 10 is a data constructional diagram showing a format of the assignment assuring message;

Fig. 11 is a detailed flowchart for a B/L storing process;

Fig. 12 is a flowchart for processes which are executed when a B/L received from another computer system is transferred to further another computer system;

Fig. 13 is a data constructional diagram showing a construction of a B/L message at a circulating or distributing stage;

Fig. 14 is a data constructional diagram showing a construction of an agreement message at the circulating stage; and

Fig. 15 is a data constructional diagram showing a construction of an assignment assuring message at the circulating stage.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0019] An embodiment of the invention will now be described in detail hereinbelow with reference to the drawings.

[0020] Fig. 1 is a block diagram showing a construction of a system in an embodiment of a data interchange system to which a data interchange method according to the invention is applied. In the embodiment, a trade and finance system for digitally interchanging Bill of Lading (B/L) as a kind of valuable papers in the trade and finance will be described as an example.

[0021] As shown in Fig. 1, a plurality of computer systems 10 to 40 which are operated by a plurality of parties regarding the trade and finance such as bank, trading company, shipping company, and the like are mutually connected to the present system through a network 50. Besides various information regarding the trade and finance, the interchange of the B/L is performed between the computer systems through the network 50.

[0022] As computer systems 10 to 40, computers such as personal computers, workstations, or the like which are generally and widely used at present can be used. Those computers can be constructed by a so-called mainframe computer of a larger scale or can be constructed as a computer system comprising a plurality of computers connected via an LAN or the like in each party where the computers are provided so long as they can realize the functions as computer systems, which will be explained hereinlater. The computer systems which are connected to the network 50 are not limited to the four systems as shown in the diagram but an arbitrary number of computer systems can be connected.

[0023] Fig. 2 is a block diagram showing a construction of a computer system. In Fig. 2, a construction of the computer system 10 provided for the bank is shown as an example and the computer systems 20 to 40 provided for the other parties are also similarly constructed. In the diagram, in the embodiment, functional constructions which are necessary for interchanging B/L among the computer systems are shown. The computer system 10 can also have functions for the other bank business. This point is also similarly applied to the computer systems provided for the parties other than the bank. The functions which are not directly concerned with the invention are not particularly shown in the diagrams and their descriptions are also omitted.

[0024] As shown in Fig. 2, the computer system 10 comprises: a processing unit 100; a memory 110; a storage device 120 represented by a magnetic disk device; a communication control unit 130; an input unit 140 such as keyboard, mouse, or the like; an output unit 150 such as CRT display, liquid crystal display (LCD), or the like; and an IC card reader/writer (IC card R/W) 160.

[0025] A certificate check program 112, a data interchange program 115, and a control program 117 have been stored in the memory 110. The processing unit 100 realizes various processes, which will be explained hereinlater, by executing those programs stored in the memory 110.

[0026] The certificate check program 112 is a program to realize a process to check the authentication of the B/L which is interchanged among the computer systems. The data interchange program 115 causes to interchange B/L which is performed among the computer systems. The control program 117 manages: an input of data from the input unit 140 by the user; an output of information to the output unit 150; an access to the storage device 120; reading/writing operations of data in an IC card through the IC card R/W; a transmission and reception of data to/from other computer systems through the communication control unit 130; and the like.

[0027] Certificate data 125 has been stored in the storage device 120. The certificate data 125 is issued from a third party such as certification authority (CA), registration authority (RA), or the like and is information to objectively certify the owner of the certificate data 125. In this case, the certificate data 125 is data which has been digitally signed by the third party to a public key information (hereinbelow, simply referred to as a public key) corresponding to a private key that is used by a party which receives a certificate.

[0028] In the embodiment, although the certificate data 125 is stored in the storage device 120 different

from the memory 110 in which the program has been stored, it can be stored in the same memory as that of the program.

[0029] Fig. 3 is a block diagram of an IC card which is owned by each party of the bank, trading company, and shipping company and is used to interchange and hold the B/L in the embodiment.

[0030] An IC card 300 has a processing unit 310, a memory 320, and an interface 330. A private key information (hereinbelow, simply referred to as a private key) 322 which is used when the party who has the IC card sends its own B/L to another party and a B/L 325 in which the party has the right are stored in the memory 320. The memory 320 includes a digital signature creation and check program 323 as functionally describe here. An IC card control program 327 for managing the private key 322 of the party and the B/L 325 in the IC card 300 and controlling an interchange of data between the computer systems through the interface 330 has been stored in the memory 320. The processing unit 310 executes the IC card control program 327, thereby controlling the management of various information in the IC card 300 and the interchange of information between the computer systems.

[0031] In the subsequent description, when the computer system provided for each party and the IC card owned by each party are mentioned, it is assumed that the reference numerals used in Figs. 2 and 3 are used in common.

[0032] Prior to describing the process for interchanging the B/L in the embodiment, a flow of the whole transaction in the trade and finance will now be explained simply.

[0033] In the trade and finance, a contract of trade is first made between the exporter and the importer.

[0034] At a point when freight to be subsequently exported is loaded to a ship for conveying, the shipping company issues a valuable paper (B/L) to accurately express a state of freight and decide the owner of the freight and passes it to the exporter. The exporter takes the B/L to a bank on the export side and requests to buy or collect it. In case of buying it, the exporter receives the cost for freight when the B/L is transferred.

[0035] The bank on the export side sends the obtained B/L to a bank on the import side. In this case, a settlement is performed even between the banks. The bank on the import side transfers the B/L in accordance with the payment of the importer. The importer receives the freight in exchange for the B/L when a ship in which the freight has been loaded enters a port.

[0036] In the trading transaction, there are various forms including a settlement method for buying and collecting and the settlement methods, timings, and the like are different. When attention is paid to a flow of the B/L, a fundamental flow is as mentioned above.

[0037] Fig. 4 is a flowchart showing a flow of processes which are executed when B/L data is newly formed in the shipping company computer system 40 and the formed B/L is transferred to the bank computer system 10. In Fig. 4, the left side shows the flow for processes which are executed by the shipping company computer system 40 serving as an issuing source of the B/L and the right side shows the flow for processes which are executed by the bank computer system 10 serving as an interchange destination of the B/L in parallel with them. In Fig. 4, an arrow shown by a broken line indicates a transfer of a message between the shipping company computer system 40 and the bank computer system 10.

[0038] First, in the shipping company computer system 40, an input of data from the input unit 140, specifically speaking, an input of the contents of the freight loaded in the ship and information showing their states is received. B/L data having the information as B/L is formed on the basis of the inputted information. (step 400).

[0039] On the basis of the formed B/L, the shipping company computer system 40 forms a B/L message which is transferred to the bank computer system 10 (step 402). The formed B/L message is sent to the bank computer system 10 by the communication control unit 130 through the network 50 (step 404).

[0040] The bank computer system 10 receives the B/L message via the communication control unit 130 (step 450). In the bank computer system 10, a signature validity check of the B/L message is performed by the certificate check program and the contents of the interchange data included in the B/L message are displayed to the output unit 150. When an acknowledgment input regarding the contents of the contract by the user on the receiving side is received, an agreement message showing that the user agrees with the contents is formed by the data interchange program 115 (step 452). The formed agreement message is sent to the shipping company computer system 40 by the communication control unit 130 via the network 50 (step 454).

[0041] The shipping company computer system 40 receives the agreement message via the communication control unit 130 (step 406). The shipping company computer system 40 checks the validation of the received agreement message by the certificate check program 112. Assignment assuring message which is held as B/L in the bank computer system 10 is formed by the data interchange program 115 (step 408). The assignment assuring message is a message to assure that the B/L was assigned from the shipping company to the bank and the message itself indicates a valuable paper data. After that, the assignment assuring message is sent to the bank computer system 10 by the communication control unit 130 via the network 50 (step 410).

[0042] When the bank computer system 10 receives the assignment assuring message (step 456), the received agreement message is finally stored and held and held as B/L into the IC card by the data interchange program 115 (step 458). An end message indic-

ative of the completion of the interchange of the B/L is sent to the shipping company computer system 40 and the processing routine is finished (step 460).

[0043] When the end message is received from the bank computer system 10 (step 412), the shipping company computer system 40 deletes the B/L data owned by itself and finishes the processing routine (step 414).

[0044] Fig. 5 is a detailed flowchart for the forming process of the B/L message which is performed in step 402.

[0045] Upon formation of the B/L message, first, the control program 117 receives an input of a scheduled interchange day of the B/L and a name of an interchange destination from the input unit 140 (step 500). The scheduled interchange day and the name of the interchange destination which were inputted are added to the B/L data which is sent to the computer system of the interchange destination by the data interchange program 115 (step 502).

[0046] After that, a digital signature is made to the interchange data comprising the B/L data, the scheduled interchange day, and the name of the interchange destination. In the embodiment, the digital signature is made by the IC card 300 owned by the operator of the present system. For this purpose, the interchange data is once stored in the IC card 300. In the IC card 300, a hash value of the interchange data is obtained by using a predetermined hash algorithm (function). The hash value is enciphered by the private key 322 and resultant information is used as a digital signature. The hash algorithm is a function which can be unconditionally coupled to the original data and form data whose size was reduced. In the embodiment, by forming the digital signature as mentioned above, the sender assures the contents of the information which is interchanged (step 504).

[0047] The data which is digitally signed by the IC card 300 is again read out by the computer system. The certificate data 125 held in the storage device 120 is added to the data by the data interchange program 115 and the B/L message is formed (step 506).

[0048] Fig. 6 shows a data format of the B/L message which is sent to the bank computer system 10 on the receiving side from the shipping company computer system 40 as a sending side of the B/L formed in step 402. A B/L message 600 includes: a B/L data field 602 having information as inherent B/L; a scheduled interchange day field 604 in which a scheduled interchange day of the B/L from the shipping company to the bank has been set; an interchange destination name field 606 in which the name of a trading company as an interchange destination is set; a first digital signature field 608 of transmitting source in which a first digital signature of the shipping company as a transmitting source is set; and a certificate field 610 of transmitting source in which a certificate of the shipping company as a transmitting source is set. As mentioned above, the first digital signature field 608 of transmitting source is data in which interchange data comprising the B/L data field 602, scheduled interchange day field 604, and interchange destination name field 606 has been enciphered by the private key 322.

[0049] Fig. 7 is a detailed flowchart for the forming process of the agreement message which is executed in step 452.

[0050] In the forming process of the agreement message, whether the certificate data set in the transmitting source certificate field 610 of the B/L message 600 sent from the transmitting source of the B/L is valid or not is first checked by the certificate check program 112. This check is performed by using the public key corresponding to the private key of the third party such as a CA/RA which issued the certificate (step 700).

[0051] Further, whether the digital signature of the transmitter set in the transmitting source first digital signature field 608 of the B/L message 600 is valid or not is checked. This check is performed by comparing the hash value obtained by deciphering the digital signature by using the public key of the transmitter calculated from the certificate with the hash value obtained from the interchange data comprising the B/L data field 602, scheduled interchange day field 604, and interchange destination name field 606 (step 702).

[0052] The data interchange program 115 checks whether the certificate data and the first digital signature are valid or not as results of the checks in steps 700 and 702 (step 704). As a result, if the certificate data or the first digital signature is not valid, an error process is performed in step 706 and the processing routine is finished.

[0053] When the authentication of the B/L message is checked in step 704, the data interchange program 115 outputs the interchange data, namely, the B/L data, the scheduled interchange day, and the name of the interchange destination to the output unit 150 (step 708). An input of the agreement data regarding the contract contents by the user (in this case, the bank is shown as an example) is received from the input unit 140. When a message indicative of a refusal of the display contents is inputted by the user, the data interchange program 115 notifies the computer system of the transmitting source of the refusal of the reception of the B/L as an error process. In this instance, for example, it is also possible to receive refusal reasons as an input from the input unit 140 and transmit it to the computer system of the transmitting source together with the interchange data (step 710).

[0054] Once the user has checked the interchange data, additional information such as image data of a handwriting signature, change data of the scheduled interchange day, or the like is added to the received B/L message as necessary (step 712). After that, in a manner similar to steps 504 and 506 in the forming process of the B/L message, a digital signature is made to the agreement data comprising the B/L message and the additional information by using the IC card 300 (step

714). Thereafter, certificate data is added and the agreement message is formed (step 716).

[0055] Fig. 8 is a data constructional diagram showing a format of the agreement message which is transferred from the computer system of the interchange destination of the B/L to the computer system of the sending source in step 454.

[0056] An agreement message 800 is constructed by adding the following data to the B/L message 600 received from the transmitting source: namely, an interchange destination additional data field 802 in which a handwriting signature or the data of the scheduled interchange day, or the like which is added on the interchange destination side is set; an interchange destination digital signature field 804 in which digital signature data of the interchange destination is set; and an interchange destination certificate field 806 in which the certificate of the interchange destination is set. The digital signature data which is set to the interchange destination digital signature field 804 is the data in which the B/L message 600 obtained by a predetermined hash algorithm and the hash value of the interchange destination additional data field 802 was encrypted by the private key 322 of the interchange destination.

[0057] Fig. 9 is a detailed flowchart for the forming process of the assignment assuring message which is executed in step 408.

[0058] In the forming process of the assignment assuring message, first, whether the certificate data set in the interchange destination certificate field 806 of the agreement message 800 sent from the interchange destination of the B/L is valid or not is checked by the certificate check program 112. This check is performed by using the public key corresponding to the private key of the third party which issued the certificate (step 900).

[0059] Further, whether the digital signature of the interchange destination set in the interchange destination digital signature field 804 of the agreement message 800 is valid or not is checked. This check is performed by comparing the hash value obtained by decrypting the digital signature by using the public key of the transmitter obtained from the certificate with the hash value calculated from the data comprising the B/L message field 600 and interchange destination additional data field 802 (step 902).

[0060] The data interchange program 115 checks whether the certificate data and digital signature of the interchange destination are valid or not as results of the checks in steps 900 and 902 (step 904). When either the certificate data or the digital signature is invalid as a result of the validation check, an error process is executed in step 906 and the processing routine is finished.

[0061] If the authentication of the agreement message is checked in step 904, the data interchange program 115 receives a decided interchange day which is inputted from the input unit 140 by the user (in this case, the shipping company is shown as an example) through the control program 117. The data interchange program 115 adds the received decided interchange day to the received agreement message 800 (step 908).

[0062] Subsequently, in a manner similar to step 504 or 714, a digital signature, namely, a second digital signature of the transmitting source is made by using the private key of the transmitting source to the data comprising the agreement message and the decided interchange day by the IC card 300 (step 910).

[0063] After that, the data interchange program 115 forms the assignment assuring message by adding additional information such as advertisement information or the like to the data to which the second digital signature was made as necessary. The additional information is not essential information in the interchange of the B/L but information such that there is no need to deny for the interchange destination (step 912).

[0064] Fig. 10 shows a data format of the assignment assuring message formed as mentioned above. As shown in the diagram, an assignment assuring message 1000 is constructed by adding the following data to the agreement message 800 sent from the interchange destination of the B/L: namely, a decided interchange day field 1002 in which the decided interchange day is set; a transmitting source second digital signature field 1004 in which the second digital signature of the transmitting source is set; and an additional information field 1006 in which the additional information is set. The digital signature data which is set to the transmitting source second digital signature field 1004 is the data in which the agreement message 800 obtained by the predetermined hash algorithm and the hash value of the decided interchange day field 1002 were encrypted by the private key 322 of the transmitting source.

[0065] The data interchange program 115 instructs the writing of the formed assignment assuring message to the IC card 300 by the IC card reader/writer 160 through the control program 117. When the assignment assuring message in which the writing was instructed is received, the IC card control program 327 of the IC card 300 checks that the first digital signature 608 and the second digital signature 1004 of the transmitting source are encrypted by the same private key 322. If this check is valid, the IC card control program 327 stores the received assignment assuring message into the memory 320, then notifies the computer system at the end of the storing process (step 914).

[0066] When the program has notified the end of the data storing process is received from the IC card 300, the data interchange program 115 confirms the two digital signatures has been created by the same private key. Then, a transmitting process of the assignment assuring message is started. After that, the IC card locks the assignment assuring message stored in the memory 320 and inhibits the subsequent accesses (step 916). The assignment assuring message stored in the memory 320 on the forming side is deleted in step 414 after the reception of the end message in step 412.

[0067] Fig. 11 shows a detailed flowchart of the B/L

storing process which is executed in step 458.

[0068] In the storing process of the B/L, whether the second digital signature of the transmitting source set in the transmitting source second digital signature field 1004 of the assignment assuring message 1000 sent from the transmitting source is valid or not is checked. This check is performed by comparing the hash value obtained by decrypting the digital signature by using the public key of the transmitter used in step 702 with the hash value calculated from the data comprising the agreement message field 800 and decided interchange day field 1002 (step 1100).

[0069] The data interchange program 115 checks whether the second digital signature of the transmitting source is valid or not as a result of the check (step 1102). If the digital signature is invalid, an error process is executed in step 1104 and the processing routine is finished. If the second digital signature is valid, the data interchange program 115 sends the assignment assuring message 1000 to the IC card 300 through the control program 117 and instructs its storage (step 1106).

[0070] In a manner similar to step 914, when the assignment assuring message 1000 is received, the IC card control program 327 of the IC card 300 on the receiving side (the bank is shown as an example) checks whether the first digital signature 608 of the transmitting source included in the assignment assuring message 1000 and second digital signature 1004 of the transmitting source are created by the same private key, or not. Whether the interchange destination digital signature field 804 is its own digital signature or not is also checked (step 1108).

[0071] When the check is made with respect to the digital signature, the IC card control program 327 stores the assignment assuring message 1000 as a B/L into the B/L storing field 325 in the memory 320 and notifies the computer system of the end of the process (step 1110). When this notice is received, the computer system executes the transmitting process of the end message in step 460 (Fig. 4).

[0072] Subsequently, processes in the case where the received B/L is further transferred to another computer system will be described. Fig. 12 shows a flowchart for processes which are executed in the case where the B/L received from the other computer system is transferred to further another computer system. In Fig. 12, the left side shows a flow for the processes which are executed by the computer system as a transmitting source of the B/L and the right side shows a flow for the processes which are executed by the computer system as an interchange destination of the B/L in parallel with the processes shown on the left side.

[0073] In response to an interchange instruction of the B/L which is inputted from the input unit 140, the data interchange program 115 starts the interchange process of the B/L stored in the IC card 300 (step 1200).

[0074] When the interchange instruction is received, the data interchange program 115 reads out the B/L held in the B/L storing field 325 in the memory 320 from the IC card 300 through the control program 117 (step 1202). The B/L which is read out here is the assignment assuring message transferred to the computer system as a transmitting source from the other computer system. For example, in case of the computer system which received the interchange of the B/L from the computer system of the issuing source, the B/L is the data that is expressed by the format shown in Fig. 10.

[0075] The data interchange program 115 of the transmitting source system forms the B/L message from the read-out B/L (step 1204). In a manner similar to step 402 (Fig. 4), the forming process of the B/L message is executed in accordance with the flowchart as shown in Fig. 5. It differs from step 402 with respect to a point that the source data to which the interchange destination name, the digital signature, and the like are added is the assignment assuring message transferred from the other computer system (corresponds to that of the trading company here) and a point that the process in step 506 of adding the certificate data in Fig. 5 is not performed. Since the B/L that is sent here has already included the certificate of the computer system as a transmitting source as a result of the process for previously receiving the B/L from the other computer system, the process in step 506 can be omitted. The other points are not particularly different from those in step 402 and their detailed descriptions are omitted here.

[0076] The data interchange program 115 transfers the formed B/L message to the computer system of the interchange destination through the network 50 (step 1206).

[0077] In the computer system of the interchange destination, when the transferred B/L message is received (step 1250), the data interchange program 115 forms the agreement message in accordance with the flowchart shown in Fig. 7 in a manner similar to step 452. As for the processes here, the check about the validity check is made in steps 700 and 702 in Fig. 7 with regard to all of the certificates and digital signatures included in the B/L message. The other processes are similar to those in step 454 described before in Fig. 7 and their descriptions are omitted here (step 1252).

[0078] The agreement message formed in step 1252 is sent to the computer system of the transmitting source of the B/L through the network 50 (step 1254).

[0079] In the computer system of the transmitting source, when the agreement message is received (step 1208), the validity check of the received agreement message of the interchange destination is made by the certificate check program 112. When the validity is checked, the assignment assuring message held as a B/L in the computer system of the interchange destination is formed by the data interchange program 115. This process is similar to that in the flowchart shown in Fig. 9. (step 1210)

[0080] After that, the assignment assuring mes-

sage is transferred to the computer system of the interchange destination by the communication control unit 130 via the network 50 (step 1212).

[0081] When the assignment assuring message is received (step 1256), the computer system of the interchange destination finally stores and holds the received assignment assuring message as a B/L into its own IC card by the data interchange program 115 (step 1258). The end message indicative of the completion of the interchange of the B/L is transmitted to the computer system of the transmitting source and the processing routine is finished (step 1260).

[0082] When the end message is received from the computer system of the interchange destination (step 1214), the computer system of the transmitting source deletes the B/L data owned by itself and finishes the processing routine (step 1216).

[0083] Figs. 13, 14, and 15 are data constructional diagrams showing data formats of the messages which are transferred in steps 1206, 1254, and 1212. The diagrams show each message when the bank receives the B/L issued from the shipping company and transfers it to the trading company (the trading company computer system 20).

[0084] Fig. 13 shows a construction of the B/L message which is sent from the bank computer system 10 as a transmitting source to the trading company computer system 20 as an interchange destination. The data corresponding to the assignment assuring message shown in Fig. 10 is included in a data field 1302 corresponding to the B/L field 602 of the B/L message shown in Fig. 6. The following data is included in the data field 1302: namely, a B/L field 1320 having the information of the inherent B/L; a shipping company certificate 1324 in which certificates of the shipping company as an issuing source; a bank certificate 1328 in which certificate of the bank as a present transmitting source has been set; a first digital signature 1322 (corresponding to the transmitting source first digital signature 608 in Fig. 6) of the shipping company used when the B/L is interchanged between the shipping company and the bank; a first digital signature 1326 (corresponding to the interchange destination digital signature 804 in Fig. 8) of the bank; and a second digital signature 1330 (corresponding to the transmitting source second digital signature 1004 in Fig. 9) of the shipping company.

[0085] A scheduled day of the interchange of the B/L from the trading company to the shipping company is set as a scheduled interchange day 1304. The name of the shipping company as an interchange destination of the B/L is set as an interchange destination name 1306. The digital signature created by the private key of the trading company is set in a transmitting source digital signature 1308. The digital signature 1308 of the transmitting source is a digital signature that is made to the B/L at the second time by the trading company and can be regarded as a second digital signature for the trading company.

[0086] Fig. 14 shows the agreement message which is sent from the computer system of the trading company to the computer system of the bank. An agreement message 1400 is constructed by adding the following data to a B/L message 1300 shown in Fig. 13: that is, interchange destination additional data 1402 which is added by the trading company; a digital signature 1404 of the interchange destination made by the trading company; and an interchange destination certificate 1406 as a certificate of the trading company.

[0087] Fig. 15 shows a data format of the assignment assuring message which is transferred from the computer system of the bank to the computer system of the trading company. An assignment assuring message 1500 is constructed by adding the following data to the agreement message shown in Fig. 14: namely, a decided interchange day 1502 from the bank to the trading company; a second digital signature 1504 of the bank as a transmitting source; and additional information 1506 which is added by the bank. The second digital signature of the transmitting source becomes a third digital signature which is made by the bank by passing through all of the messages.

[0088] Although the above embodiment has been described with respect to the interchange of the B/L among three parties, the B/L can be sequentially circulated among a larger number of parties by repeating the processes described in Fig. 12.

[0089] According to the system described in the embodiment, after checking the contents of the information that is transmitted at the stage where the B/L message is received, the interchange destination of the B/L can refuse the reception of it if necessary. Since the received B/L message is incomplete as a B/L to be circulated, the operation such that the interchange destination illegally uses the received information in spite of a fact that it refused the information can be avoided. Thus, when the B/L is circulated, the reliability can be improved without needing a center-like system which manages the circulation of the B/L.

[0090] In the embodiment described above, three digital signatures are added to the message by the party concerned with the interchange each time the B/L is transferred. Therefore, while the B/L is sequentially circulated, the number of digital signatures to be checked increases and much time is required for processes. To avoid such a problem, a process when the B/L received from another company is transferred to further another company can be changed as follows.

[0091] First, in step 1204 in Fig. 12, the B/L message is formed without the digital signature of the transmitting source and transferred to the computer system of the interchange destination. Therefore, the message that is transferred to the computer system of the interchange destination becomes a message without the digital signature 1308 of the transmitting source from the message shown in Fig. 13.

[0092] In the computer system of the interchange

destination, after the validation was sequentially checked with respect to the digital signatures in the message in B/L storing step 1252, for example, at the stage (step 710 in Fig. 7) where the agreement of the information is obtained from the user, the preceding second digital signature of the transmitting source added to the preceding assignment assuring message by the transmitting source of the B/L owned by the transmitting source at this time point is deleted. Predetermined data is added to the data in this state, thereby forming the agreement message.

[0093] Moreover, in the computer system of the interchange destination, in step 1258, as a check of the digital signatures included in the assignment assuring message, its own digital signature added at the second order from the last is validity-checked, and whether the last digital signature and the digital signature added at the third order from the last, namely, the digital signature added to the assignment assuring message by the transmitting source computer system and the digital signature added to the assignment assuring message transferred to the transmitter when the transmitting source computer system receives the B/L are digitally signed by the same private key or not is checked.

[0094] By the above processes, the agreement message becomes a message without a digital signature field 1330 and the digital signature field 1308 (refer to Fig. 13) from the data field 1302 in the message shown in Fig. 14. Similarly, the agreement message becomes a message without the digital signature field 1330 and digital signature field 1308 (refer to Fig. 13) from the data field 1302 in the message shown in Fig. 15.

[0095] By the above processes, the number of digital signatures of the party who owned the B/L at the halfway stage can be set to one and the number of digital signatures in the message can be reduced as compared with that in the foregoing embodiment. Even if the number of times of transmutation increases, a large increase in processing time can be prevented.

[0096] The network is used for transfer of the B/L in the embodiment described above. Although a transmutation might be troublesome, a storage medium such as floppy disk, magnetic tape, or the like, for example, can be also used in place of the network. When the digital signature is made, it is also possible to construct the system so that the hash value is calculated in each computer system, the obtained hash value is inputted to the IC card, and the digital signature is made.

[0097] The information that is stored in the IC card is not limited to the whole digital signature target data but can be set only to the digital signature data, and the actual information can be stored in the storage device of the computer system.

[0098] Further, as for the data which is not concerned with the digital signature of the transmitter in the data in each message, it is possible to delete such data on the receiving side and then form the next message.

[0099] Moreover, as a specific example, an example of the circulation among the three parties such that the shipping company generates the right and transfers it to the bank and the bank transfers it to the trading company has been described in the embodiment. However, the invention is not limited to the circulation of the data among the three parties but the right can be sequentially circulated by repeating the data transfer process between the bank and the trading company described as an example. In this instance, the digital signatures in the message can be also used as history information of the transmutation of the right.

[0100] The certificate that is used in the embodiment does not depend on the certificate issuer. Therefore, when the digital signature made finally in the assignment assuring message and the digital signatures (the first digital signature of the transmitting source and the second digital signature of the transmitting source) made at the third order from the last are checked as to if these digital signatures are made by the same party, different certificates can be also used to check each digital signature. In this case, each time the digital signature is made and the message is sent to the partner, it is sufficient that the person who makes the digital signature allows the certificate corresponding to the digital signature made at this time to be included in the message. By this method, the certificates issued from a plurality of authorities can be also used together.

[0101] The invention is not limited to the circulation of the B/L in the trade and finance system as mentioned above but can be widely applied to the transfer of the data such as various digital documents or the like which are circulated among a plurality of parties.

[0102] In the above embodiments, the executing steps in each of the computer system of the data transmitting source and the computer system of the interchange destination shown in Figs. 4 and 12 can be stored as a form of program codes into a recording medium such as semiconductor memory, floppy disk, CD-ROM, or the like. In place of them, programs for executing the processing steps can be also loaded into each computer through a communication line.

[0103] According to the invention, the interchange of the digital documents among a plurality of parties can be performed while assuring the contents. The circulation of the digital document whose contents need to be assured can be realized without intervening a third party-like system serving as a center, for example, a third trust party (TTP).

Claims

1. A data interchange method for interchanging data among a plurality of computers (10, 20, 30, 40) through a network (50), comprising the steps of:

   in a first computer as a transmitting source of said data, forming a first message obtained by

adding a first digital signature to indicate validation of said data and transferring said first message to a second computer;
in said second computer, checking validation of said first message on the basis of said first digital signature;
in said second computer, forming a second message by adding a second digital signature to indicate validation of said first message to the first message and transferring said second message to said first computer;
in said first computer, checking validation of said second message on the basis of said second digital signature;
in said first computer, forming a third message by adding a third digital signature to indicate validation of said second message to the second message and transferring said third message to said second computer; and
in said second computer, checking validation of said third message on the basis of said third digital signature and holding said third message as data to be received from said first computer.

2. A method according to claim 1, wherein in a process to form said second message, said data is outputted to an output unit (150) and said second message is formed in accordance with information which is inputted from an input unit (140) in response to the output of said data.

3. A method according to claim 1, wherein

a process to form said first message has a step of adding a certificate to indicate that a transmitting source of said first message is said first computer to said data, and
a process to form said second message has a step of adding a certificate to indicate that a transmitting source of said second message is said second computer.

4. A method according to claim 1, further comprising the steps of:

in said second computer, forming a fourth message by adding a fourth digital signature to indicate validation of said third message to the third message and transferring said fourth message to a third computer;
in said third computer, checking validation of said fourth message on the basis of the digital signature included in said fourth message;
in said third computer, forming a fifth message by adding a fifth digital signature to indicate validation of said fourth message to the fourth message and transferring said fifth message to said second computer;
in said second computer, checking validation of said fifth message on the basis of said fifth digital signature;
in said second computer, forming a sixth message by adding a sixth digital signature to indicate validation of said fifth message to the fifth message and transferring said sixth message to said third computer; and
in said third computer, checking validation of said sixth message on the basis of said sixth digital signature and holding said sixth message as data to be received from said second computer.

5. A method according to claim 1, further comprising the steps of:

in said second computer, forming a fourth message to be transferred to a third computer on the basis of said third message and transferring said fourth message to said third computer;
in said third computer, forming a fifth message by adding a fifth digital signature to indicate validation of said fourth message to the data excluding said third digital signature included in said fourth message and transferring said fifth message to said second computer;
in said second computer, checking validation of said fifth message on the basis of said fifth digital signature;
in said second computer, forming a sixth message by adding a sixth digital signature to indicate validation of said fifth message to the fifth message and transferring said sixth message to said third computer; and
in said third computer, checking validation of said sixth message on the basis of said sixth digital signature and holding said sixth message as data to be received from said second computer.

6. A data interchange system which comprises a first computer (10, 20, 30, 40), a second computer (10, 20, 30, 40), and a network (50) to transmit data between said first and second computers and interchanges a digital document through said network, wherein:

said first computer includes means (323) for forming a first message by adding a first digital signature to indicate validation of document data which is transferred to said second computer to said document data and transferring said first message through said network;
said second computer includes means (323) for checking validation of said first message on

the basis of said first digital signature and means (323) for forming a second message by adding a second digital signature to indicate validation of said first message to the first message and transferring said second message to said first computer;

said first computer further includes means (323) for checking validation of said second message on the basis of said second digital signature and means (323) for forming a third message by adding a third digital signature to indicate validation of said second message to the second message and transferring said third message to said second computer; and

said second computer further includes means (323) for checking validation of said third message on the basis of said third digital signature and memory means (325) for holding said third message.

7. A system according to claim 6, wherein

said second computer includes an output unit (150) to display information and an input unit (140) to receive an input from the user, and

said means for forming and transferring said second message outputs said document data to said output unit and forms said second message in accordance with information that is inputted from said input unit in response to the output of said data.

8. A system according to claim 6, wherein

said first computer includes means (323) for adding a certificate to indicate that a transmitting source of said first message is said first computer to said first message, and

said second computer includes means (323) for adding a certificate to indicate that a transmitting source of said second message is said second computer to said second message.

9. A system according to claim 6, further comprising a third computer, and

wherein:

said second computer includes means (323) for forming a fourth message by adding a fourth digital signature to indicate validation of said third message and transferring said fourth message to said third computer;

said third computer includes means (323) for checking validation of said fourth message on the basis of the digital signature included in said fourth message and means (323) for forming a fifth message by adding a fifth digital signature to indicate validation of said fourth message to the fourth message and transferring said fifth message to said second computer;

said second computer further includes means (323) for checking validation of said fifth message on the basis of said fifth digital signature and means (323) for forming a sixth message by adding a sixth digital signature to indicate validation of said fifth message to the fifth message and transferring said sixth message to said third computer; and

said third computer further includes means (323) for checking validation of said sixth message on the basis of said sixth digital signature and memory means (325) for holding said sixth message.

10. A system according to claim 6, further comprising a third computer, and

wherein:

said second computer includes means (323) for forming a fourth message to be transferred to said third computer on the basis of said third message and transferring said fourth message to said third computer;

said third computer includes means (323) for forming a fifth message by adding a fifth digital signature to indicate validation of said fourth message to the data excluding said third digital signature included in said fourth message and transferring said fifth message to said second computer;

said second computer further includes means (323) for checking validation of said fifth message on the basis of said fifth digital signature and means (323) for forming a sixth message by adding a sixth digital signature to indicate validation of said fifth message to the fifth message and transferring said sixth message to said third computer; and

said third computer further has means (323) for checking validation of said sixth message on the basis of said sixth digital signature and memory means (325) for holding said sixth message.

11. A memory medium which stores a program that is executed by a computer in order to interchange digital data among computers (10, 20, 30, 40) through a network (50), wherein said program comprises the steps of:

forming a first message obtained by adding a first digital signature to indicate validation of data to said data;

transferring said first message to another computer through said network;

receiving a second message which includes said first message and to which a second digital signature to indicate validation of said first message has been added by said another computer;
checking validation of said second message on the basis of said second digital signature; and
forming a third message by adding a third digital signature to indicate validation of said second message to the second message and transferring said third message to said another computer.

12. A memory medium which stores a program that is executed by a computer in order to interchange digital data among computers (10, 20, 30, 40) through a network (50), wherein said program comprises the steps of:

receiving a first message including said digital data from another computer and a first digital signature added to said digital data to indicate validation of said digital data by said another computer;
checking validation of said digital data on the basis of said first digital signature;
forming a second message by adding a second digital signature to indicate validation of said first message to the first message;
transmitting said second message to said another computer;
by said another computer, receiving a third message which includes said second message and to which a third digital signature to indicate validation of said second message has been added by said another computer; and
storing and holding said third message into a memory device (320).

13. A medium according to claim 12, wherein said program further comprises the steps of:

transferring said third message to further another computer through said network;
receiving a fourth message which includes said third message and to which a fourth digital signature to indicate validation of said third message has been added by said further another computer;
checking validation of said fourth message on the basis of said fourth digital signature; and
forming a fifth message by adding a fifth digital signature to indicate validation of said fourth message to the fourth message and transferring said fifth message to said another computer.

14. A medium according to claim 13, wherein said step of transferring said third message to said further another computer includes a step of adding a sixth digital signature to said third message.

15. A medium according to claim 12, wherein said step of checking the validation of said digital data includes a step of, in the case where a plurality of digital signatures are included in said first message, deleting a message finally added to said first message.

16. A medium according to claim 12, wherein said step of forming said second message includes a step of outputting contents of said digital data to an output unit (150) and a step of receiving a check reply from the user which is inputted from an input unit (140) in accordance with a result of said output.

17. A data processing method for a first party constructing a data transmitting source to sequentially interchange data among computers (10, 20, 30, 40) of at least the first party and a second party through a network or a digital medium (300), comprising the steps of:

by using the computer of said first party as a transmitting source of said data, forming a first message in which a first digital signature to indicate validation of said data has been added to said data and transferring said first message to the computer of said second party;
receiving, from said second party, a second message in which validation of said first message is checked on the basis of said first digital signature and adding a second digital signature to indicate validation of said first message has been added to the first message by the computer of said second party; and
checking validation of said received second message on the basis of said second digital signature, forming a third message by adding a third digital signature to indicate validation of said second message to the second message, and transferring said third message to the computer of said second party; and
thereby, causing the computer of said second party to check validation of said third message on the basis of said third digital signature and enable said third message to be held as data to be received from said first computer.

18. A method according to claim 17, wherein said first to third messages include data which have been irreversibly compressed and are transferred between said first and second parties without an intervening party.

19. A data processing method for a second party con-

structing a receiving source to sequentially interchange data among computers (10, 20, 30, 40) of at least a first party and the second party through a network or a digital medium (50, 300), comprising the steps of:

receiving a first message formed by adding a first digital signature to indicate validation of said data to the data by the computer of said first party as a transmitting source of said data;
by using the computer of the second party checking validation of said received first message on the basis of said first digital signature, forming a second message by adding a second digital signature to indicate validation of said first message to the first message, and transferring said second message to the computer of said first party;
receiving a third message formed by checking validation of said second message on the basis of said second digital signature and then adding a third digital signature to indicate an assurance of validation of said second message to the second message by the computer of said first party; and
checking validation of said received third message on the basis of said third digital signature and holding said third message as data to be received from the computer of said first party.

20. A method according to claim 19, wherein in a process to form said second message, said data is outputted to an output unit (150) and said second message indicative of an agreement is formed in accordance with information that is inputted from an input unit (140) in response to the output of said data.

21. A method according to claim 1, wherein said network is formed of a digital medium (300).

22. A computer-executable program for implementing a digital signature-based data processing for a first party constructing a data transmitting source to sequentially interchange data among computers (10, 20, 30, 40) of at least the first party and a second party through a data transmission means (50, 300), said program executing the steps of:

by using the computer of said first party as a transmitting source of said data, forming a first message in which a first digital signature to indicate validation of said data has been added to said data and transferring said first message to the computer of said second party;
receiving, from said second party, a second message in which validation of said first message is checked on the basis of said first digital signature and a second digital signature to indicate validation of said first message has been added to the first message by the computer of said second party; and
checking validation of said received second message on the basis of said second digital signature, forming a third message by adding a third digital signature to indicate validation of said second message to the second message, and transferring said third message to the computer of said second party; and
thereby, causing the computer of said second party to check validation of said third message on the basis of said third digital signature and enable said third message to be held as data to be received from said first computer.

23. A program according to claim 22, wherein said first to third messages include data which have been irreversibly compressed and are transferred between said first and second parties without an intervening party.

24. A computer-executable program for implementing a digital signature-based data processing for a second party constructing a receiving source to sequentially interchange data among computers (10, 20, 30, 40) of at least a first party and the second party through a data transmission means (300, 50), said program executing the steps of:

receiving a first message formed by adding a first digital signature to indicate validation of said data to the data by the computer of said first party as a transmitting source of said data;
by using the computer of the second party, checking validation of said received first message on the basis of said first digital signature, forming a second message by adding a second digital signature to indicate validation of said first message to the first message, and sending said second message to the computer of said first party;
receiving a third message formed by checking validation of said second message on the basis of said second digital signature and then adding a third digital signature to indicate an assurance of validation of said second message to the second message by the computer of said first party; and
checking validation of said received third message on the basis of said third digital signature and holding said third message as data to be received from the computer of said first party.

25. A program according to claim 24, wherein in a process to form said second message, said data is outputted to an output unit (150) and said second

message indicative of an agreement is formed in accordance with information that is inputted from an input unit (140) in response to the output of said data.

FIG. 1

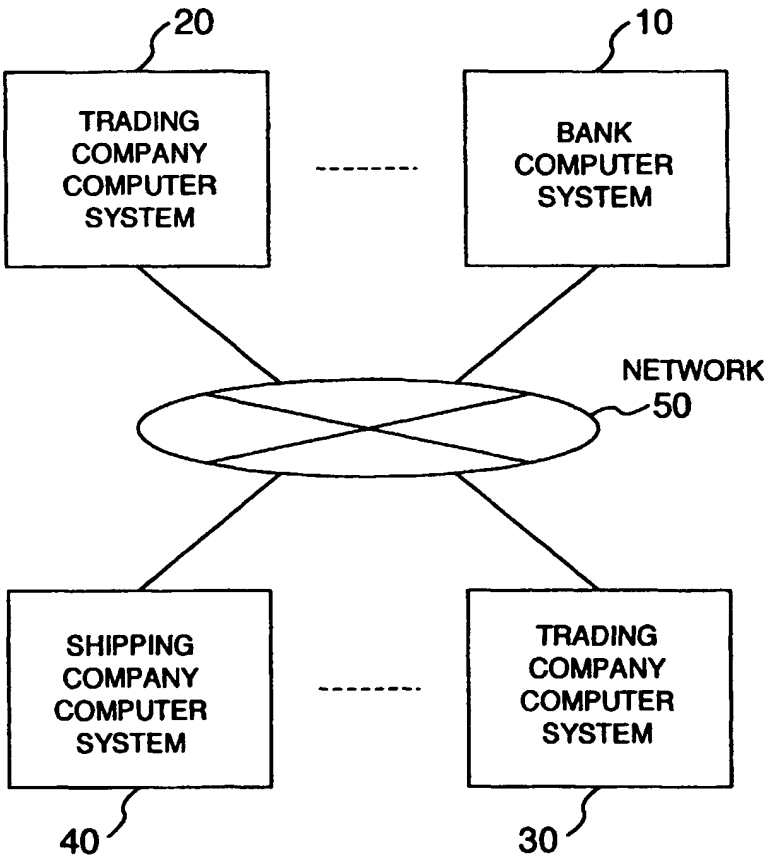

20
10
TRADING COMPANY COMPUTER SYSTEM
BANK COMPUTER SYSTEM
NETWORK
50
SHIPPING COMPANY COMPUTER SYSTEM
TRADING COMPANY COMPUTER SYSTEM
40
30

FIG. 2

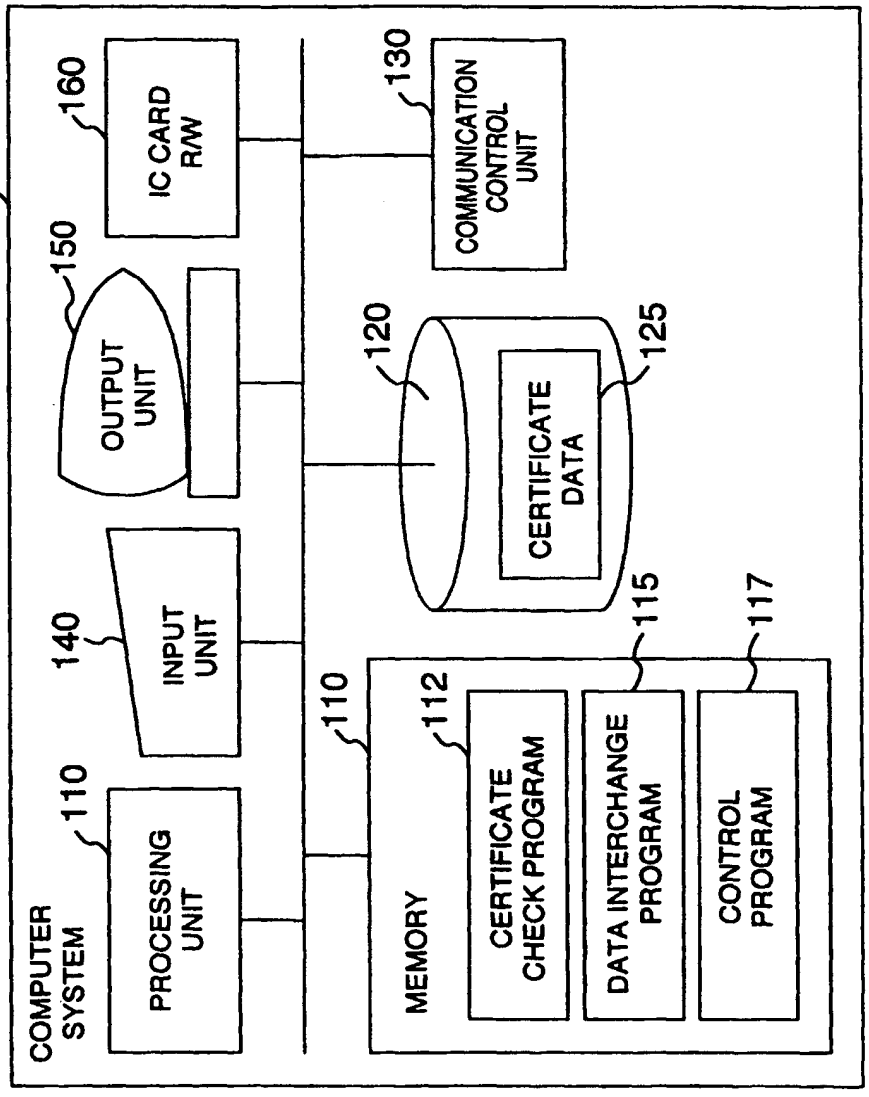

10
COMPUTER SYSTEM
110
PROCESSING UNIT
140
INPUT UNIT
150
OUTPUT UNIT
160
IC CARD R/W
130
COMMUNICATION CONTROL UNIT
110
MEMORY
112
CERTIFICATE CHECK PROGRAM
115
DATA INTERCHANGE PROGRAM
117
CONTROL PROGRAM
120
CERTIFICATE DATA
125

FIG. 3

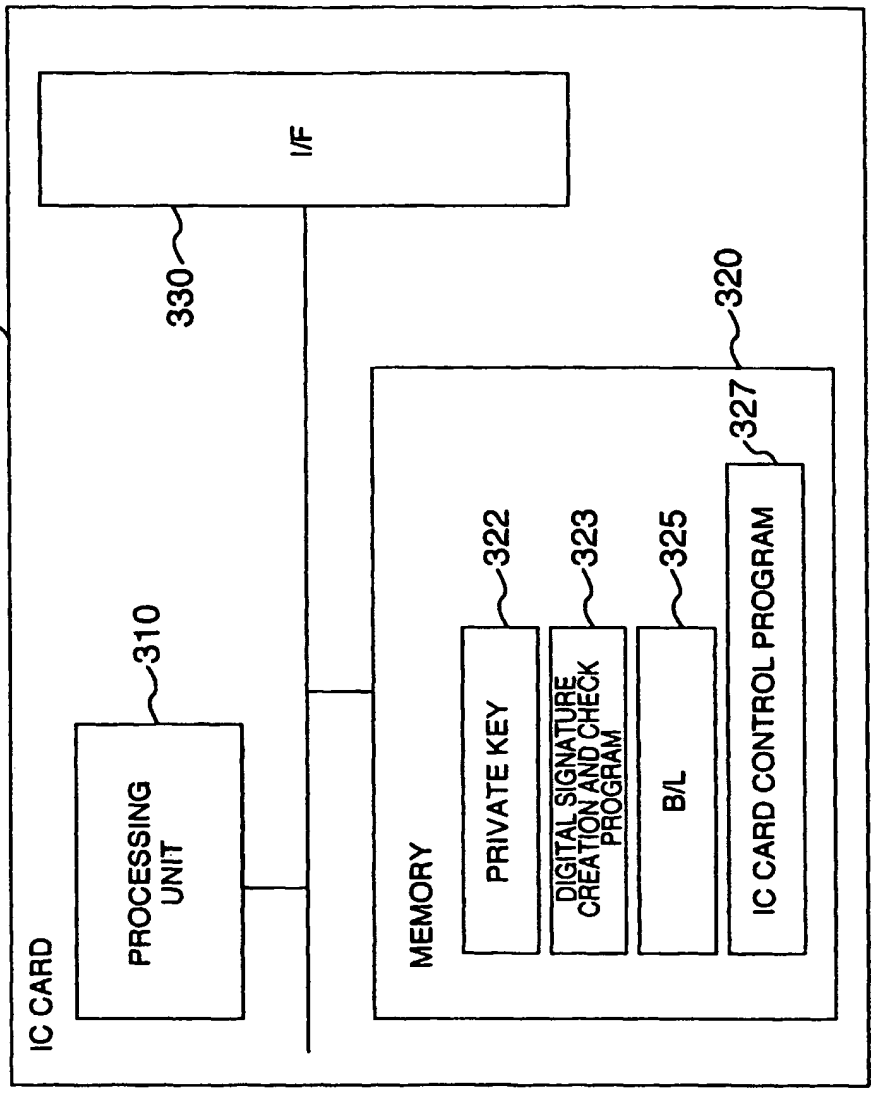

IC CARD
300
PROCESSING UNIT
310
I/F
330
MEMORY
320
PRIVATE KEY
322
DIGITAL SIGNATURE CREATION AND CHECK PROGRAM
323
B/L
325
IC CARD CONTROL PROGRAM
327

FIG. 4

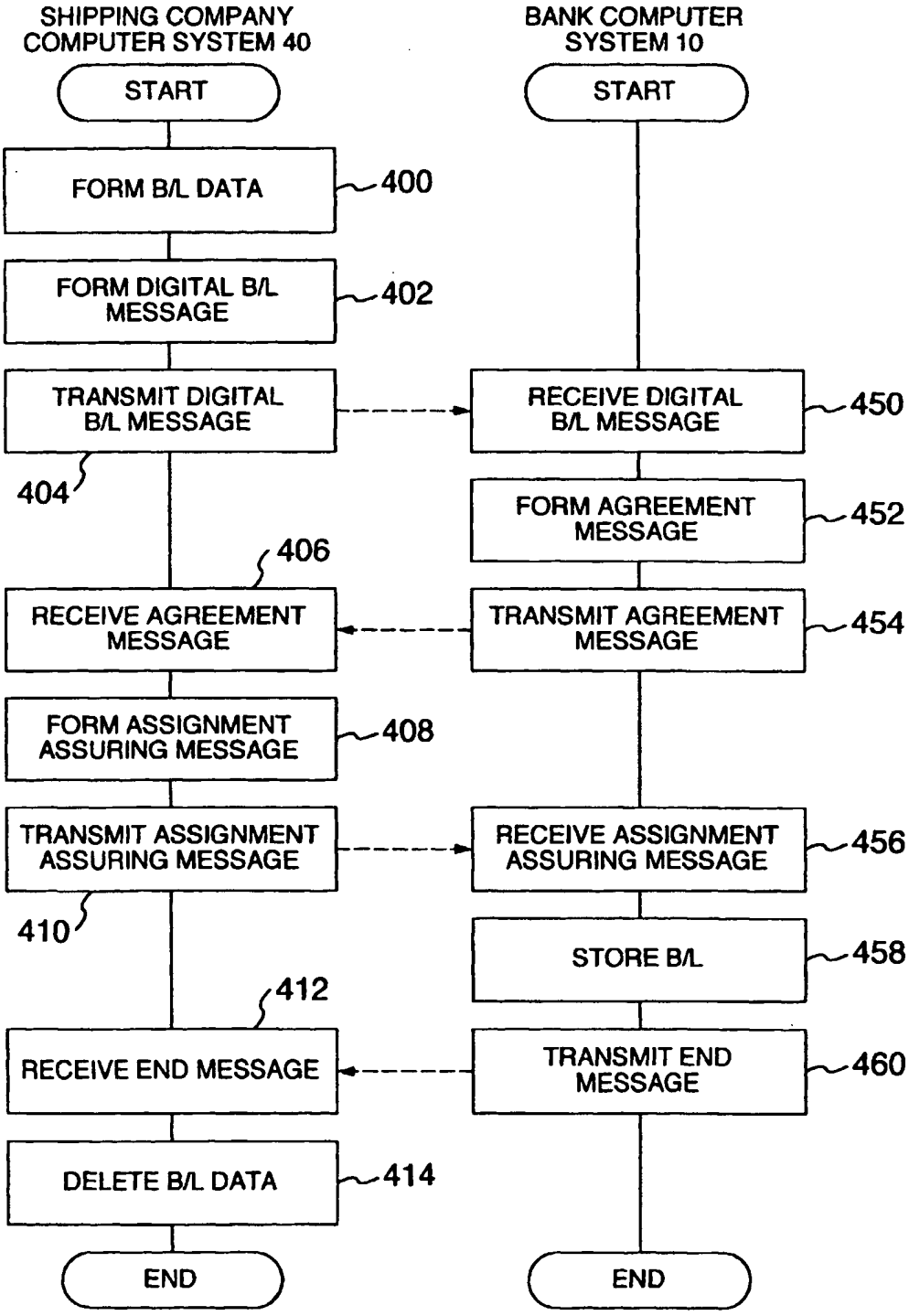

SHIPPING COMPANY COMPUTER SYSTEM 40
BANK COMPUTER SYSTEM 10
START
START
FORM B/L DATA
400
FORM DIGITAL B/L MESSAGE
402
TRANSMIT DIGITAL B/L MESSAGE
RECEIVE DIGITAL B/L MESSAGE
450
404
FORM AGREEMENT MESSAGE
452
406
RECEIVE AGREEMENT MESSAGE
TRANSMIT AGREEMENT MESSAGE
454
FORM ASSIGNMENT ASSURING MESSAGE
408
TRANSMIT ASSIGNMENT ASSURING MESSAGE
RECEIVE ASSIGNMENT ASSURING MESSAGE
456
410
STORE B/L
458
412
RECEIVE END MESSAGE
TRANSMIT END MESSAGE
460
DELETE B/L DATA
414
END
END

FIG. 5

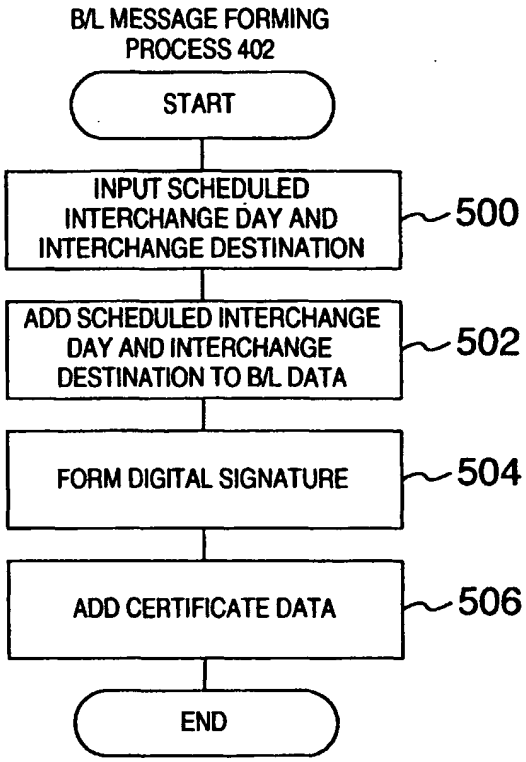

B/L MESSAGE FORMING PROCESS 402
START
INPUT SCHEDULED INTERCHANGE DAY AND INTERCHANGE DESTINATION
500
ADD SCHEDULED INTERCHANGE DAY AND INTERCHANGE DESTINATION TO B/L DATA
502
FORM DIGITAL SIGNATURE
504
ADD CERTIFICATE DATA
506
END

FIG. 6

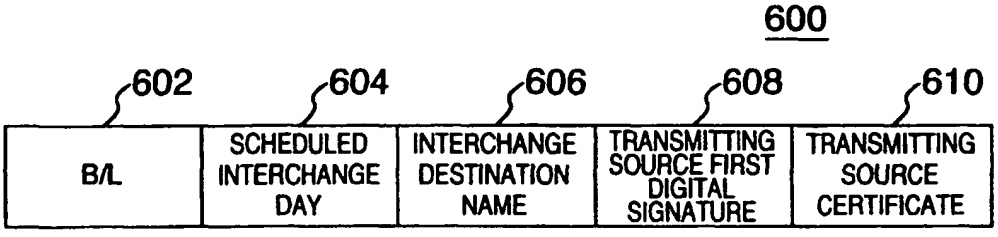

600
602
604
606
608
610
B/L
SCHEDULED INTERCHANGE DAY
INTERCHANGE DESTINATION NAME
TRANSMITTING SOURCE FIRST DIGITAL SIGNATURE
TRANSMITTING SOURCE CERTIFICATE

FIG. 7

RECEIVING SIDE AGREEMENT MESSAGE FORMING PROCESS 452

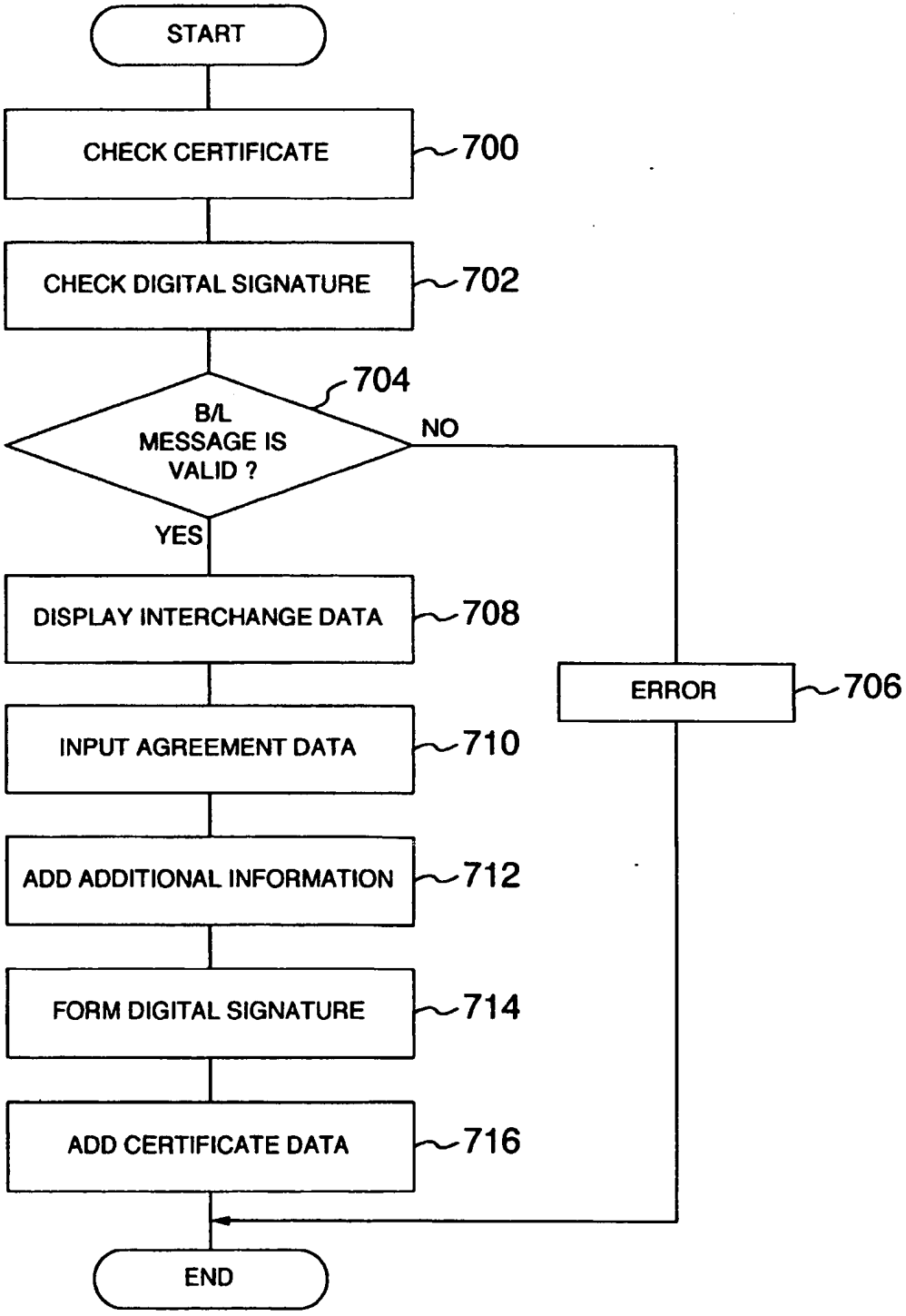


FIG. 8

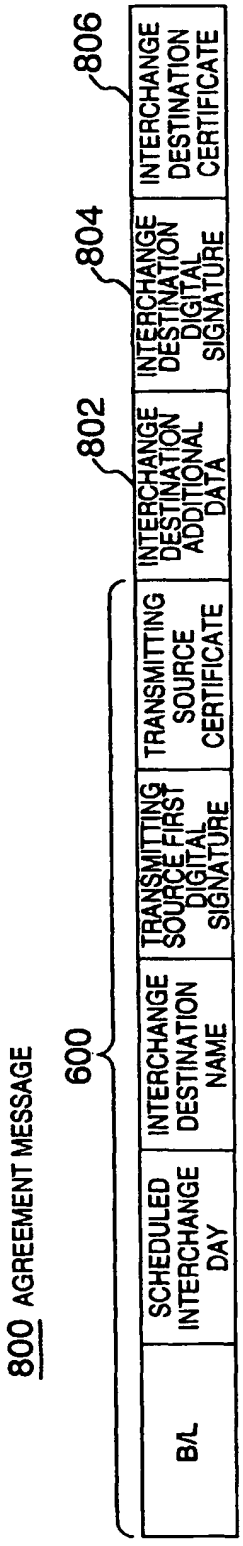

800 AGREEMENT MESSAGE
600
B/L
SCHEDULED INTERCHANGE DAY
INTERCHANGE DESTINATION NAME
TRANSMITTING SOURCE FIRST DIGITAL SIGNATURE
TRANSMITTING SOURCE CERTIFICATE
INTERCHANGE DESTINATION ADDITIONAL DATA
802
INTERCHANGE DESTINATION DIGITAL SIGNATURE
804
INTERCHANGE DESTINATION CERTIFICATE
806

FIG. 10

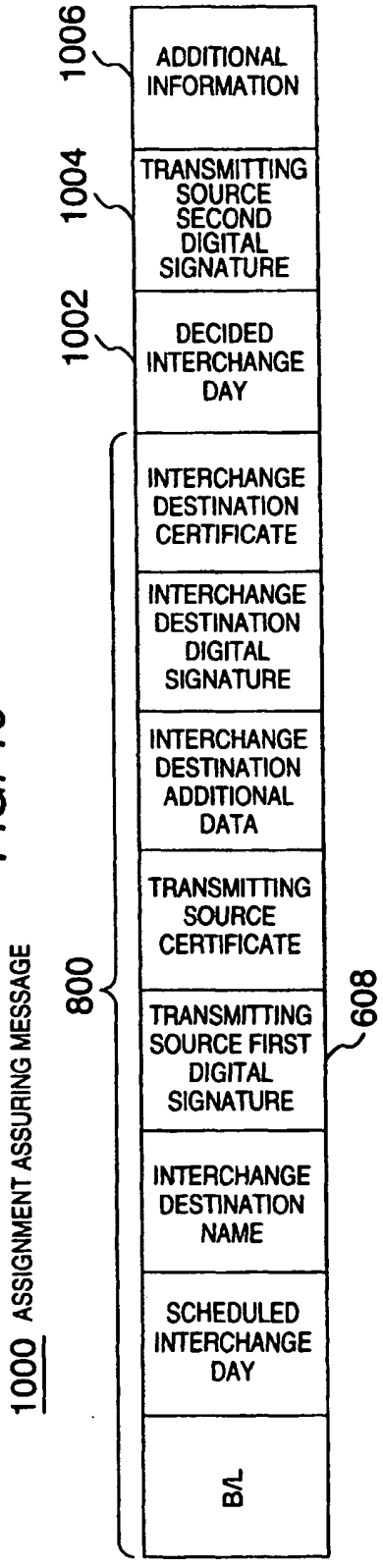

1000 ASSIGNMENT ASSURING MESSAGE
800
B/L
SCHEDULED INTERCHANGE DAY
INTERCHANGE DESTINATION NAME
TRANSMITTING SOURCE FIRST DIGITAL SIGNATURE
608
TRANSMITTING SOURCE CERTIFICATE
INTERCHANGE DESTINATION ADDITIONAL DATA
INTERCHANGE DESTINATION DIGITAL SIGNATURE
INTERCHANGE DESTINATION CERTIFICATE
DECIDED INTERCHANGE DAY
1002
TRANSMITTING SOURCE SECOND DIGITAL SIGNATURE
1004
ADDITIONAL INFORMATION
1006

FIG. 9

ASSIGNMENT ASSURING MESSAGE FORMING PROCESS 408

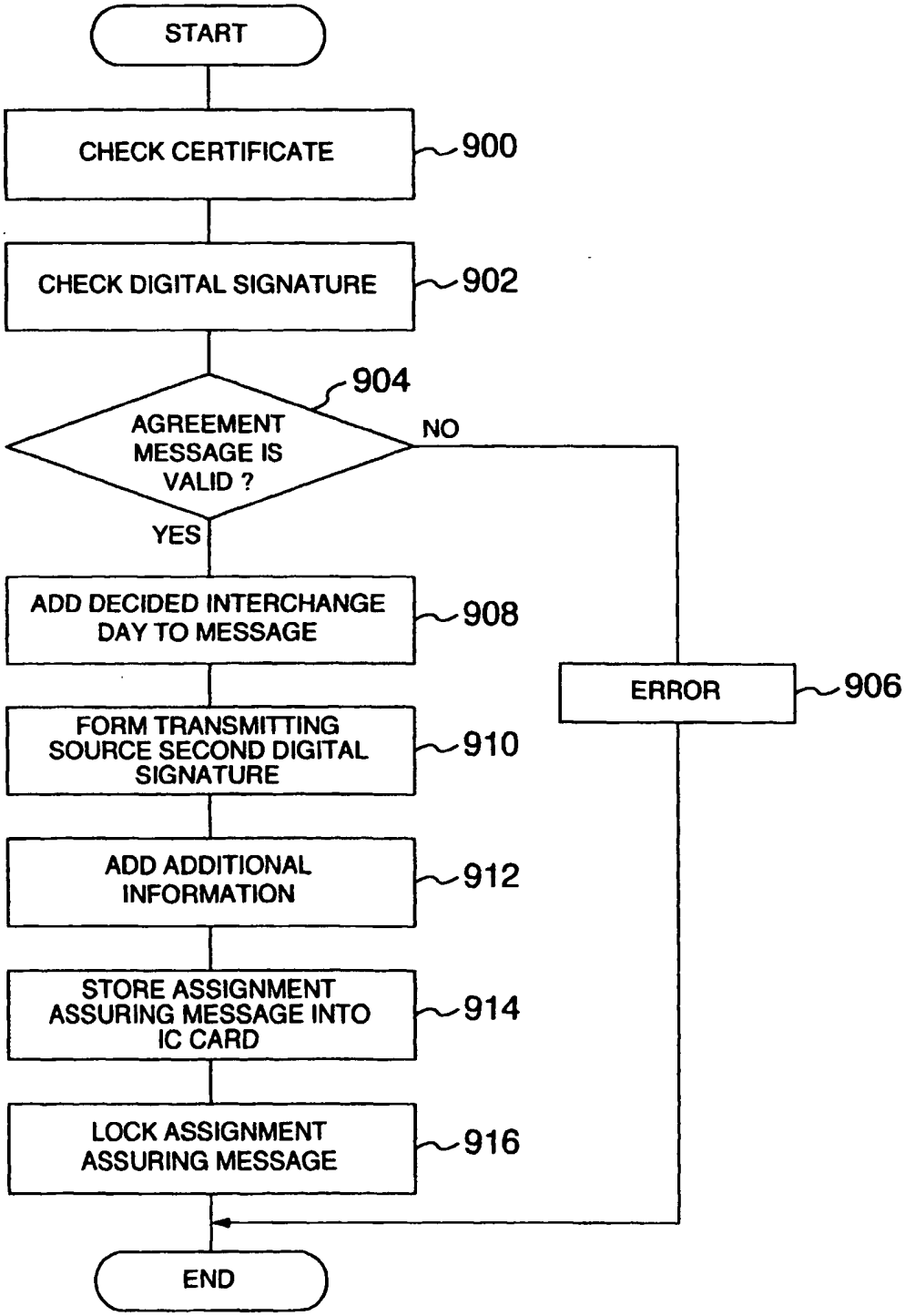


FIG. 11

B/L STORING PROCESS 458

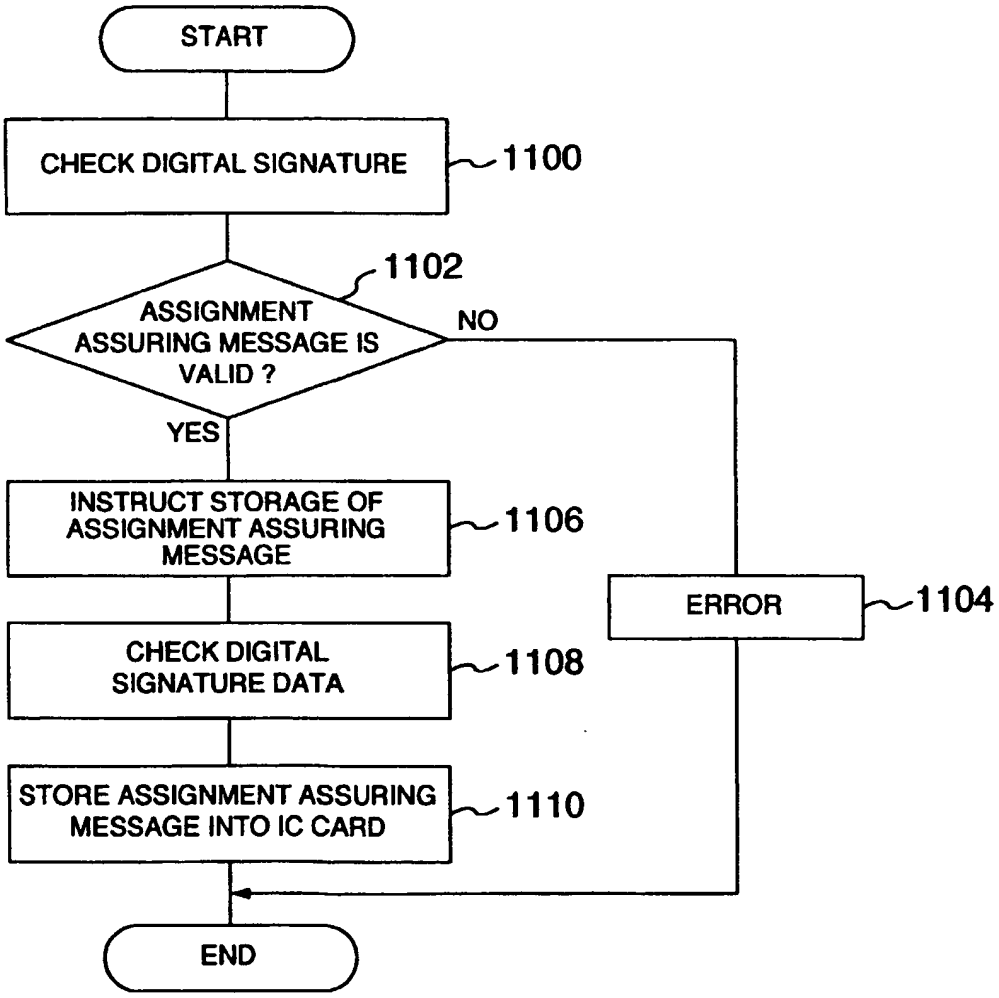


FIG. 12

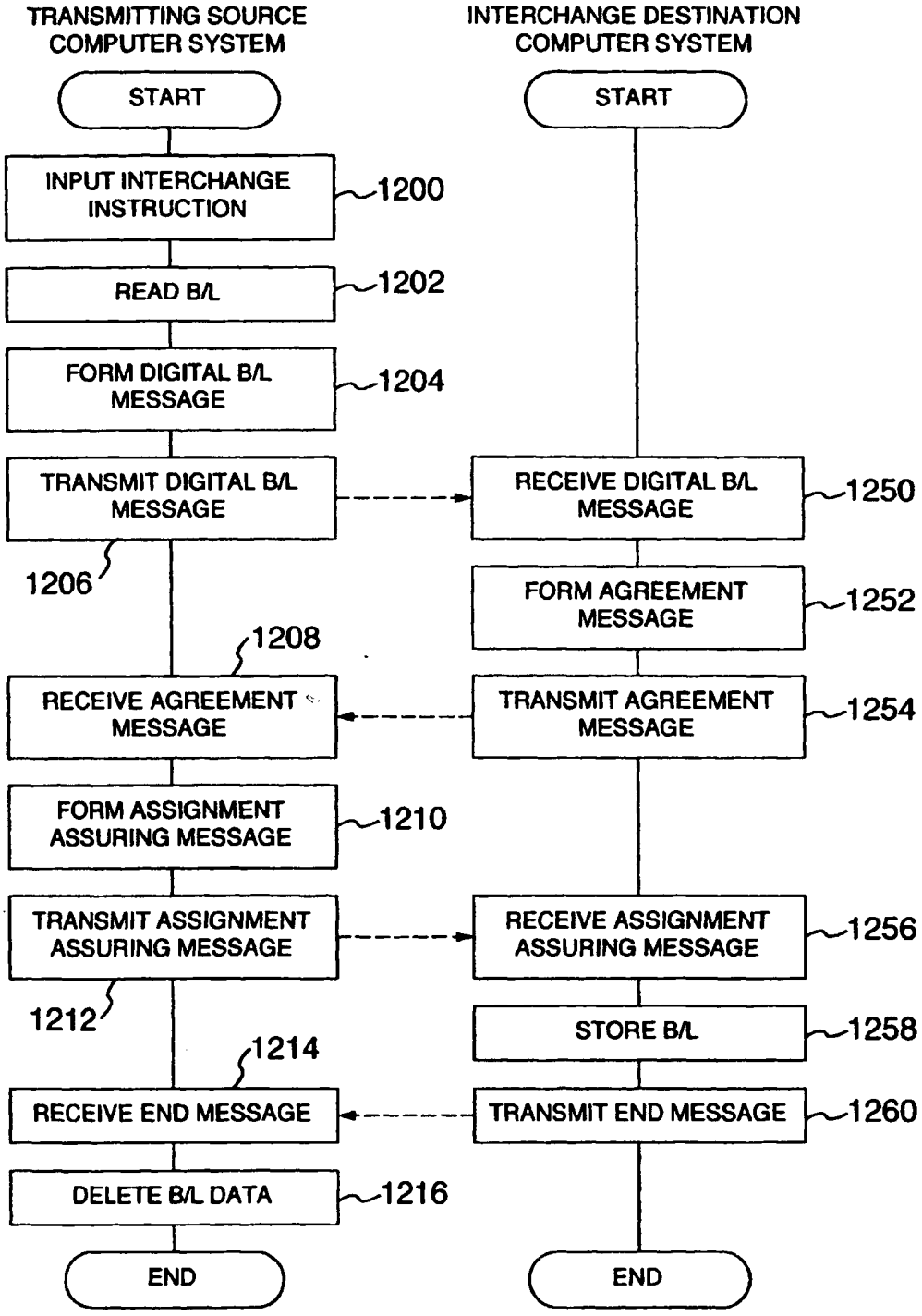

TRANSMITTING SOURCE COMPUTER SYSTEM
INTERCHANGE DESTINATION COMPUTER SYSTEM
START
START
INPUT INTERCHANGE INSTRUCTION
1200
READ B/L
1202
FORM DIGITAL B/L MESSAGE
1204
TRANSMIT DIGITAL B/L MESSAGE
RECEIVE DIGITAL B/L MESSAGE
1250
1206
FORM AGREEMENT MESSAGE
1252
1208
RECEIVE AGREEMENT MESSAGE
TRANSMIT AGREEMENT MESSAGE
1254
FORM ASSIGNMENT ASSURING MESSAGE
1210
TRANSMIT ASSIGNMENT ASSURING MESSAGE
RECEIVE ASSIGNMENT ASSURING MESSAGE
1256
1212
STORE B/L
1258
1214
RECEIVE END MESSAGE
TRANSMIT END MESSAGE
1260
DELETE B/L DATA
1216
END
END

FIG. 13

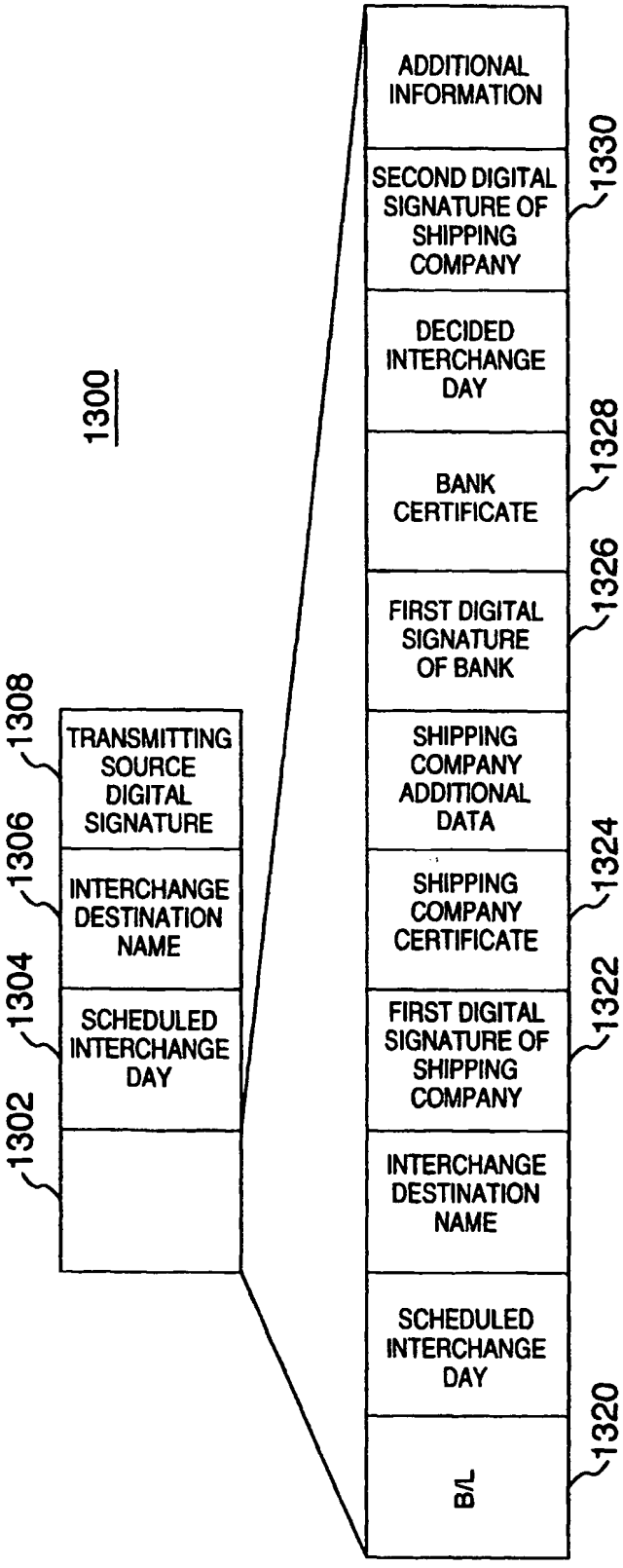

1300
1308
TRANSMITTING SOURCE DIGITAL SIGNATURE
1306
INTERCHANGE DESTINATION NAME
1304
SCHEDULED INTERCHANGE DAY
1302
ADDITIONAL INFORMATION
SECOND DIGITAL SIGNATURE OF SHIPPING COMPANY
1330
DECIDED INTERCHANGE DAY
BANK CERTIFICATE
1328
FIRST DIGITAL SIGNATURE OF BANK
1326
SHIPPING COMPANY ADDITIONAL DATA
SHIPPING COMPANY CERTIFICATE
1324
FIRST DIGITAL SIGNATURE OF SHIPPING COMPANY
1322
INTERCHANGE DESTINATION NAME
SCHEDULED INTERCHANGE DAY
B/L
1320

FIG. 14

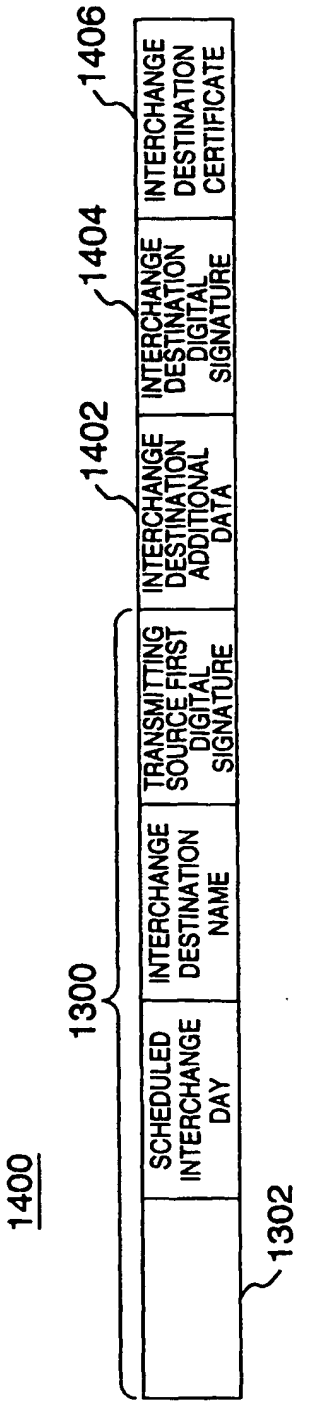
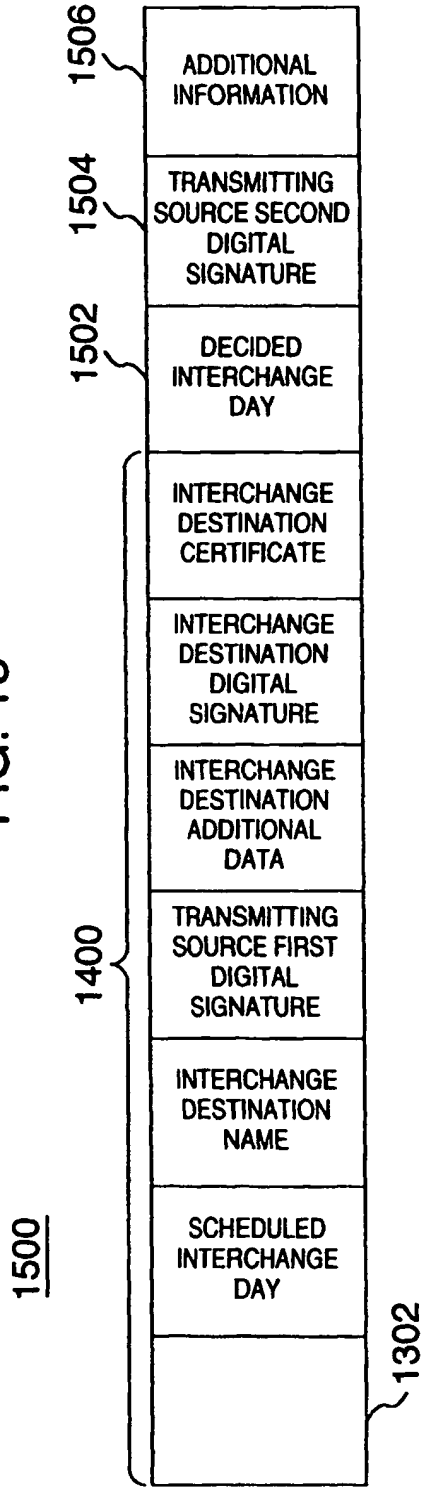

1400
1300
1302
SCHEDULED INTERCHANGE DAY
INTERCHANGE DESTINATION NAME
TRANSMITTING SOURCE FIRST DIGITAL SIGNATURE
INTERCHANGE DESTINATION ADDITIONAL DATA
1402
INTERCHANGE DESTINATION DIGITAL SIGNATURE
1404
INTERCHANGE DESTINATION CERTIFICATE
1406

FIG. 15


1500
1400
1302
SCHEDULED INTERCHANGE DAY
INTERCHANGE DESTINATION NAME
TRANSMITTING SOURCE FIRST DIGITAL SIGNATURE
INTERCHANGE DESTINATION ADDITIONAL DATA
INTERCHANGE DESTINATION DIGITAL SIGNATURE
INTERCHANGE DESTINATION CERTIFICATE
1502
DECIDED INTERCHANGE DAY
1504
TRANSMITTING SOURCE SECOND DIGITAL SIGNATURE
1506
ADDITIONAL INFORMATION